STAT INT

ARTICLE APPEARED
ON PAGE C-2

WASHINGTON TIMES
8 December 1983

A U.S. intelligence vacuum?

ALLAN BROWNFELD

The terrorist bombing of the U.S. Marine headquarters in Beirut and the unexpectedly large Cuban presence that American forces found in Grenada have raised major questions about the performance of our intelligence agencies.

The intelligence questions, according to Reagan administration officials and members of Congress, revolve around two immediate concerns: whether better intelligence information might have helped prevent the attack on the Marines in Beirut on Oct. 23 and whether the American troops that invaded Grenada two days later were sufficiently informed about the strength of Cuban forces on the island.

The officials said that fundamental questions also had been raised about the mission and methods of the nation's intelligence agencies, including the issue of whether U.S. spying had become too dependent on sophisticated electronic surveillance equipment instead of human agents.

Military officers who commanded the invasion of Grenada complain about an intelligence vacuum that they say left assault forces unprepared for the stiff resistance they encountered from Cuban troops.

In Lebanon, U.S. officials report that intelligence tended to lack the specific information that would enable the authorities to block assassination plots or other terrorist activities. Three days before a terrorist drove the truck filled with tons of explosives into the Marine headquarters in Beirut, killing 240 American servicemen, the Central Intelligence Agency reported that a pro-Iranian Moslem splinter group appeared to be planning an attack against the Marines. The report was widely distributed among senior government officials, including Marine leaders.

Defenders of the CIA cite the report as evidence that the agency provided at least some warning before the bombing, even if it did not give the time, target or type of attack. Gen. Paul X. Kelley, the Marine commandant, disputed that suggestion, telling members of the House Armed Services Committee that no one had given the Marines the kind of detailed intelligence they needed to prevent a suicide bombing attack. "I'm not talking about those broad, vague, general statements that they hide behind," Gen. Kelley said, in an apparent reference to the Oct. 20 intelligence report. "I'm talking about specificity, about a truck."

Gen. Kelley, of course, protests a bit too much. "Did he want the license plate number as well?" one intelligence official asked. Rather than denying any responsibility for lax security, Gen. Kelley would have done well to remain silent until a thorough investigation had been conducted. If the security was indeed thorough, why was it that a host of new security precautions were implemented the day after the bombing?

With regard to Grenada, Defense Department officials said they were surprised by both the number of Cuban combat forces and the extent of Soviet and Cuban influence on the island. Intelligence officials acknowledged that detailed information on both subjects was unavailable, but said that planning for the invasion had moved so rapidly that there was little time to prepare the tactical intelligence normally required for a military assault. They also said that the military services, not the CIA, were responsible for the collection of tactical intelligence.

Administration officials say the CIA had little information about political developments in Grenada. As a result, they said, Washington was caught by surprise when Prime Minister Maurice Bishop was ousted in the October coup.

In both Grenada and Lebanon, intelligence officials said, the information that was lacking was of the kind best obtained by human agents rather than satellites, reconnaisance aircraft or other electronic equipment. It was, we must remember, during the Carter administration — and the CIA directorship of Stansfield Turner, that many of our most experienced agents were released from service. "Human agents," the Carter administration told us, were no longer necessary in the new technological age. Now we can see how wrong that assessment was.

In Grenada, the CIA had no permanent presence and the State Department maintained no permanent diplomatic presence. As a result, the United States had few reliable sources of information.

The U.S. intelligence capability has been permitted to decline dramatically. In 1981, an analysis of the intelligence-gathering role of the CIA concluded that, "The American intelligence community has routinely failed to predict major political and military developments before such developments become irreversible and before they become blatantly obvious, even to the general public."

What the report called "massive and virtually inexplicable intelligence failures that occurred during the last 15 years" include failure to predict the massive Soviet buildup of nuclear missiles; failure to predict the major improvements in accuracy of Soviet ICBMs in the late 1970s; consistent gross misstatement of Soviet global objectives; general failure to explain the characteristics of Soviet conventional weapons systems and vessels, for example, the Soviet T-64 and T-72 tanks and the new Russian guided-missile cruisers; and the entire situation in Iran.

One serious defect in U.S. intelligence, critics charge, is the lack of competitive analysis and any process for quality review. Former Defense Intelligence Agency Director Daniel Graham has proposed that analysis and estimates should be carried out by competing intelligence bureaucracies with each having equal access to the president and the chief intelligence officer of the United States, who would no longer be the director of the CIA.

CONTINUED

ARTICLE APPEARED
ON PAGE 68

WASHINGTON POST MAGAZINE
4 December 1983

STATINTL [redacted]

THE ADMIRAL'S BRIEF GUIDE TO AMERICAN SPYING

Bobby Inman likes to put things in perspective, and offers a standard 20-minute review of the history of American intelligence-gathering that goes something like this:

For the first 100 years of its existence, the United States created intelligence organizations during wartime and abolished them when the wars were over. The first permanent peacetime intelligence unit was created in 1882, when the Secretary of the Navy chartered what became the Office of Naval Intelligence, and a naval officer went to England . . . to count British ships!

The Defense Department, not to be outdone, sent men to Berlin, Vienna and Petersburg, and the race was on. World War I gave impetus to the notion of gathering of technical intelligence, and by the time we entered World War II we had what Inman calls an austere intelligence gathering capability.

That ability soon became lush, with the OSS, clandestine human collection and covert action. "After the war, the leadership sat down to talk about what to do. They decided that we should never again be so dumb about the outside world." They already had Navy, Army and State Department intelligence; the CIA was to run the clandestine operations but, in a break with the British system, also had a major analytical division.

The Korean war demonstrated a need for better information flow among departments, so the director of Central Intelligence was given a leadership role, "to produce a flow to the CIA, and a reverse flow."

President Truman, wanting a separate agency for technical intelligence, chartered the secret National Security Agency in 1952. Tasking came from the director of Central Intelligence, but it was administered by the Defense Department. Collectors in the field were military; the internal staff was civilian. NSA's main purpose was to function in wartime, but things being what they are in Washington, it was soon functioning full time.

The CIA built its encyclopedic intelligence base and launched its covert activities. But in 1959 none of the intelligence agencies could agree, for instance, on how many missiles the Soviets had. Eventually, President Kennedy discovered there was indeed a missile gap—we had more than the Russians.

Kennedy's Secretary of Defense, Robert McNamara, deciding that he wanted control of analysis, commissioned the Defense Intelligence Agency. Overt operations went to the State Department, covert stayed with the CIA.

The war in Vietnam took a lot of people away from activities elsewhere in the world; then, because of the balance of payments problem, American presence abroad was reduced. That, says Inman, was "the single most damaging decision to the country's human intelligence system."

The country's technical capability was increased, with the use of satellites, but manpower on the technical side declined. Simply put, there were not enough people to sort through the material collected. One result: the Yom Kippur war in 1973 went unpredicted. Revelations of CIA misconduct and acrimonious congressional hearings damaged the reputation of intelligence gatherers of all sorts, abroad and at home.

"By 1980, there were four prospective foreign agents in America for every agent here to cover them," Inman says. The ideal ratio is two FBI agents for every suspected spy. "The total intelligence community had been reduced 40 percent since the plateau was reached in the early '60s."

The Reagan administration has reversed the trend, Inman says. □

—James Conaway

ARTICLE APPEARED
ON PAGE 19
WASHINGTON POST MAGAZINE
4 December 1983

THE INMAN FILE

BY JAMES CONAWAY

James Conaway is a staff writer for The Washington Post Magazine.

Back in 1975, when Bobby Ray Inman was director of Naval Intelligence, he was invited by some Senate staffers to come up to Capitol Hill and discuss the Soviet threat. The invitation proved to be more complicated than it appeared, as invitations to spies often do . . . but let Inman tell the story himself:

"After the meeting, a staffer asked me to lunch. We went to a little restaurant on the back side of the Hill, and two characters slid into the seats next to us. They started talking to me, suggesting that if their companies got some contracts, they could be of great help to the Navy. I was just beginning to get incensed when one of them said, 'By the way, I work for you.'"

Inman was flabbergasted. The man was Edmund Wilson, a hulking former CIA agent who belonged to the secret Naval Intelligence organization known as Task Force 157, whose members gathered intelligence about harbors around the world. While working for Task Force 157, Wilson had managed to become a rich man, owning a Virginia horse farm, among other things. He would go on to procure illegal explosives for Libyan terrorists and attempt to have some people assassinated, but that's another story.

"I went back to the office," Inman says, "and asked, 'Who is this guy?' That day I decided to terminate Wilson's contract." Inman had already decided to do away with Task Force 157, to [illegible] budgetary requirements, but the meeting with Wilson convinced him that the decision was sound. "Later"—and Inman smiles the gap-toothed smile so familiar to congressional committees and intelligence operatives—"Wilson blamed me for a lot of his troubles."

Inman was Wilson's antithesis, principled to a fault, and so physically unassuming that as a child he was often beaten up in east Texas schools (until he helped two brawny classmates with their homework and learned the value of bodyguards).

Today Wilson is in prison and Inman is drinking California riesling in the first-class cabin of a Boeing 727 streaking between Washington and Austin. "The thought crossed my mind," he says, gazing at his wan reflection in the blackened window of the aircraft, "that Wilson might try to do me harm."

Inman is a civilian now, the director of a consortium of electronics and computer companies known as MCC that is racing the Japanese toward the next generation of supercomputers. When Inman retired last year as deputy director of the Central Intelligence Agency, he probably had more varied experience in analytical intelligence than anyone. Though not a Naval Academy graduate, Inman worked his way up through Naval Intelligence to become a four-star admiral, was named deputy director of the Defense Intelligence Agency in 1976 and then became the youngest director ever of the secretive, monolithic National Security Agency.

He tried to retire in 1981, with 30 years of military service, but President Reagan personally asked him to take the number-two job under CIA director William Casey. Inman agreed, but left the CIA a year later, to critical acclaim from congressmen and soldiers alike, some of whom feared that American intelligence was losing one of its most valuable assets.

Inman resisted interviewers while in government, but decided to talk about intelligence-gathering for the simple reason that "it's an important subject." His views on the men and the machines in the business are instructive. Former CIA director William Colby says Inman "had all the jobs and never let the bureaucracy get in his way . . . He respected the congressional prerogative, but was also concerned with keeping the necessary secrets."

"He's a consummate professional and a highly moral individual," says George Carver, who was deputy of national intelligence in the CIA in the mid-1970s, now a senior fellow at the George-town Center for Strategic and International Studies. "Bobby Inman has always been an extremely articulate and able advocate of the true net interests of whatever agency he represented."

That is a fair description of a good spy.

"Articles saying that I'm a master spy are pure garbage," Inman says. "I've never run a clandestine operation. But I've been an avid user of what they produce."

Disputes over covert action were cited as the reason Inman left the CIA; however, differences between him and Casey reportedly arose from personality conflicts, rather than philosophy, and the natural differences between generations. Casey was dropping spies into Nazi Germany when Inman was a Texas whiz kid.

Computers are as essential to the government Inman worked for as they are fundamental to his new endeavor, in a world where private enterprise and government service often overlap. His competitors might well be uneasy, given the admiral's vita.

Inman insists he is no longer in *the business*: "I'm not using any clandestine or technical sources to determine what the Japanese are doing. I do know that wherever I go to speak, there are substantial Japanese in attendance."

He looks like the class valedictorian, twisting a University of Texas ring around his finger while deflating some notions about spies and technology.

CONTINUED

PERSONAL COMPUTING
December 1983

[redacted]

Talking Shop With Admiral Bobby Inman

STATINTL

Admiral Bobby Inman spent more than 22 years organizing international high-tech espionage networks for the U.S. Navy, the Defense Intelligence Agency, the CIA, and the National Security Agency, where he served as director from 1977 to 1981. Now Inman has turned from the classified to the proprietary, spearheading an unprecedented computers and semiconductor-research venture pooling the talents and money of 12 major U.S. corporate investors, the resources of the University of Texas at Austin, and some of the best scientific minds in the nation. The result is MCC—Microelectronics and Computer Technology Corporation—of which Inman, 53, is president and chief executive officer. Formed less than two years ago, the company is the brainchild of William C. Norris, chairman of Control Data Corporation, who saw the necessity of formulating a uniquely American response to Japanese high-technology initiatives, especially those government-sponsored.

"Norris began worrying about it about eight years ago when he saw the Japanese putting up money and bringing together research talent from competing companies," Bobby Inman explains. "We didn't have anything like that . . . and it was a great idea."

Unlike the cooperative fifth generation and artificial intelligence projects conducted by Japan's Ministry of International Trade and Industry and the Institute for New Generation Computer Technology, however, MCC is totally a private sector initiative; bankers, industrialists, academics, and political figures have joined together to raise private donations in addition to monies put up by the participating shareholders. These include some of the leading U.S. competitors in semiconductors and computers: Control Data Corp., Motorola Inc., Honeywell Inc., NCR, National Semiconductor Inc., RCA Corp., Sperry Corp., United Technologies Corp., Harris Corp., Digital Equipment Corp., Advanced Micro Devices, Inc., and Allied Corp. These companies will also contribute research and administrative talent to the venture.

MCC's plan is to develop proprietary designs in software, computer-aided design and manufacturing, packaging of integrated circuits, and advanced computer design, all of which can be adapted for profitable commercial product lines by the sponsoring companies. Many projects should come to fruition in six to 10 years, at which time the sponsors will get a license and a three-year jump on the marketplace.

Admitting that he is terribly excited about the prospects for MCC, Admiral Inman, one of the world's foremost intelligence experts, is also cognizant of the risks involved. Last year he gained national prominence—and drew the ire of critics—by advocating before a congressional committee that certain advanced electronics research data might be subject to some form of government review. While Inman still maintains his suggestions were blown way out of proportion by the media, he also remains firm in his belief that strategic information—and proprietary technologies—must be protected. Technological spying is on the increase all over the globe, he acknowledges. Japanese espionage, as revealed in the well-publicized IBM-Hitachi case, in which FBI men in the Silicon Valley rounded up more than a dozen businessmen working on behalf of both Hitachi and Mitsubishi Electric Companies to buy stolen secrets from IBM, may be part of an "iceberg," Inman suggests. De-

spite these problems, he argues that international alliances of the most sensitive nature must be formed and held together even as economic competition grows more heated. Inman, ever-surprising, looks highly favorably *on the Japanese and the pressures they've exerted on the American technological mind-set. Out of challenge, he argues, comes growth, and only with growth and the reassertion of America's technological leadership in the world can political stability be attained. The implications of this position are vast, and as worldly as the Admiral himself: In his interview with* Personal Computing*'s Arielle Emmett, he revealed himself to be a highly confident man with a flair for talk and the long view; for historicizing optimistically, even about the Soviets; for arching his brow when his picture was taken and for smiling when words would not take him any further. A former deputy director of the Central Intelligence Agency, Inman was guarded on particulars of national security, and of his own intelligence experience, although in a second interview, he was more open about matters of security. But his demeanor went against everything one classically thinks of as "spy." Instead, Inman traverses the world of science, of education, of politics and of shared hope for a world he believes will reap real benefits from advanced computing technologies. Below, some excerpts from two long and challenging interviews.*

Admiral Inman, the current perception is that the United States is losing ground in the international competition for supremacy in high technology industries. Why have we fallen behind?

Inman: In the immediate post-war years, a lot went into fueling the great economic boom. Education was the hero. And that happened in two ways: a very large upswing in undergraduate education as a result of the G.I. bill, and graduate education which in very large measure came from grants from the Defense Department, unrestricted, no strings attached. But in the early 1960s, we began examining defense with a new set of tools. One of the early parameters was cost-effectiveness, and a decision was made which said that it wasn't cost-effective to give grants unless they were directly tied to weapons systems or likely weapons systems. The impact of cutbacks began to show up by 1968 when there was a drop in the number of graduate students in sciences and math. The total student population in graduate schools in the U.S. did not drop because a lot of foreign students began to come in and take up the open spaces, and we trained a lot of fine scientists and sent them back to Japan and other countries along the way. So now we need to review the business of grants for graduate study, but that's going to take years. The key question is: How do you keep up with the external competition given a shortage of overall talent to take advantage of opportunities?

What kind of insights into foreign competition did you get during your years in security work?

Inman: I spent the bulk of my time looking at our principle adversaries—the Soviets—and a reasonable amount looking at the North Koreans, the Vietnamese, the evolving relationships with the Chinese, a lot less about Eastern Europe, and very little about the rest of the world. I've a lot of friendships in our allied countries. I've had the privilege of living in Japan several times, being on ships based out there, and I have lots of friends in the Japanese Navy. But I frankly know very little more than most of you who have been reading avidly what the Japanese are doing. I have an enormous admiration for what they have accomplished.

Are the Japanese conducting a form of technological espionage in this country and are we simultaneously doing that with them? They are—technically at least—our allies.

Inman: I'm reasonably comfortable with an answer that we are not conducting industrial espionage in Japan, or in Western Europe for that matter.

How about them?

Inman: Well—yeah—the Hitachi case, I don't know how big that iceberg is.

I know that over the last 10 or 12 years, we've moved towards sharing technology more with our allies. And that's largely been a defense-oriented thrust. There is also a role here that the multinational companies play in spreading technology. When you stand back to look, IBM has major investments in Japan. It's interesting that they are the target of the Hitachi efforts in this country. Yet, they've got shared research efforts with the Japanese and they've got major holdings in Japan. Texas Instruments, which is not one of my shareholders, has a number of collaborative arrangements with the Japanese. So again—don't get me into too deep trouble—I have somewhat a different view from some of my shareholders about the Japanese. I think the Japanese have shown us how to do a very efficient job of using trained power to take basic research to technology which is commercialized. They have had government funding and authority to do it. I am not recommending that we follow that model. I much prefer a private enterprise-fueled one to do it if we can. We've got to see if we can. The Japanese got past the cultural problem; they brought competitors together to do research. So I don't look at the Japanese as *the enemy*, and I take a view that competition is healthy. Now I do think that means that Japanese markets have to be opened up.

One person I spoke with who is doing systems for the U.S. military said that in the marketing of defense systems—rapid nuclear response systems, for instance—the Japanese don't distinguish between allies and adversaries.

Inman: Potential adversaries?

Right. They really will sell to anybody, this computer expert asserted to me. Is that your perception, also?

Inman: My perception has been that they were *insensitive* to potential military applications. And that's partly why the Japanese military hasn't been that good a market. So they've been out hawking the commercial market. We've left them one percent of the GNP going into their own military investment and we've not been a market for buying from the Japanese.

CONTINUED

But other countries have, I understand.

Inman: They've gone to where there was a market. And perhaps one insensitive to military applications. But in the relatively few cases I'm aware of where we've raised that question, the Japanese response has been forthcoming. So there is an education factor here.

In other words, you're saying that you can—with the right kind of cooperative relations with the Japanese, foster a better understanding of what is sensitive and what is not? And whom to sell to?

Inman: I think when you focus on the question of adversarial access, you've really got to do it in a pro-common environment, you really can't do it in a U.S.-only climate. And when the Japanese stand back and look at the adversarial side, they'll find what they usually sell is one or two or three of a kind and then they [the buyers] go build their own. When they stand back and look at it, that's not a big commercial market.

What about the Russians and the Chinese? I have read that they have stepped up their espionage, particularly in high technology areas, and as a result, a number of Soviet emissaries have been thrown out of various countries. But in this country, are we aware enough, as a nation, of security, even as it affects our particular audience—business people with computers in their offices?

Inman: We are probably the most open society in the world. And I think that is basically good. You know one of the earlier acts children learn is using the telephone. And we never give it up the whole rest of our lives. And I found that whether people were in commercial enterprise and living in foreign countries or whether they were diplomats or military officers, if they suddenly wanted to talk about something, they just grabbed the nearest phone and started talking to their American counterparts without any thought about who all else might be enjoying that conversation. And the same thing is true with the bulk of our commercial dealers.

When there is a prospect of loss of proprietary data that might make a profit, all of a sudden, some of the very best security exists in this country . . .

You know I'm a year out of date on following most of these problems. But certainly earlier in my goverment environs, and in dealing with security regularly, I've found that IBM was no slouch in industrial security. When companies believe there is a genuine prospect that they will lose business . . . they get very protective of it. There's a new complication, though, on the U.S. scene, at least certainly in the information handling industry. And that's the rapid move of venture capital to support new entrepreneurs with a new idea going out. Universities have a steady drain of talent going off from their faculties to start companies and in many cases become very wealthy and productive entrepreneurs. A lot of companies have had people break off. When we were doing site selection for MCC, I found that my shareholding companies were not at all enthused about the company going to Silicon Valley in California because of a very high turnover rate of technical personnel. You move them out there and very soon thereafter they find a venture capitalist. I've noticed with interest this past year IBM's efforts to hold former employees accountable to statements they had signed for protection of proprietary data.

Oh really?

Inman: Yes! They have taken some very aggressive moves, some lawsuits against people who have moved out and taken ideas with them.

Do you think that's a valid way of trying to exert control?

Inman: Well, we're clearly headed down that road. All MCC employees will sign a proprietary agreement. All intellectual property, all patents will belong to MCC, and they are not to share them without approval.

Did you see the copyrighted story in The New York Times ***that appeared (September 25, 1983, Sunday, "Security of Computers Worries Military Experts" by William J. Broad) discussing computer security and the penetration teams?***

Inman: No I did not.

There was material here, and . . . let me read it to you . . . about altering (computer) programs. (Here the interviewer read a few short excerpts from the article citing a case in which scientists at Bell Laboratories during the 1970s had put a security bypassing procedure into a computer program. With such a program, the computer would " . . . skip normal security procedures and immediately give access to key secrets." The Times ***reported. Although Bell Laboratory officials asserted such a program never ran outside the lab's facilities, Defense Department experts claimed that such a program in fact was "installed at different sites around the country, including the National Security Agency, which specializes in electronic espionage and runs the Pentagon computer security center," according to the article. Admiral Inman was head of the National Security Agency between 1977 and 1981.)***

Inman: The security center is actually the Department of Defense Computer Security headquarters physically located at NSA . . . It's been created over the last two years as a dedicated effort by DOD to look at the problem.

The article cites an anonymous Defense Department source who contends the program was used for roughly two years before someone discovered it. He said NSA computers weren't vulnerable unless the Bell program were connected to outside telephone lines. Are they?

Inman: To the best of my knowledge, the answer is no.

But the National Security Agency did use the Bell program?

Inman: I don't even know if they used the Bell system, but what I do know is that those are all classified computer systems. They're not the unclassified ones like you'd set up in Bell Labs . . . where you want to communicate. I don't know what they may have changed in the last couple years, but my firm recollection is that there were no computer systems (at NSA) which could be accessed by telephone.

CONTINUED

Approved For Release 2001/03/07 : CIA-RDP91-00901R000500240013-6

But are you saying there were programs at the National Security Agency computers that used a Bell system?

Inman: I don't know. I don't remember any that did.

Let's go on. This is where we talk about penetration teams. The article cites Proceedings of the United States Naval Institute. According to the Proceedings, as cited in the Times *report, "There are means at hand for saboteurs to penetrate this country's military computer systems."*

Inman: That's flatly false. I don't believe it's true at all. From a lot of years of looking at them, I think the vast bulk of suggestions about potential penetration are great flights of imagination which have no basis in fact. I don't think it's a valid threat at all.

Can I ask you one other question? Experts cited in the Times *claimed the government had engaged scientists to try to break into computers. Despite their efforts and the redesigning of security systems in recent years, NSA hasn't certified that any of its computer systems are invulnerable from internal attack. My question is . . .*

Inman: The question cited was internal attack . . . The other question is telephone access or external attack . . . And internal attack means if you've got someone who actually has physical access to the facilities and the rest of it. You know there is a vulnerability.

Did you have any involvement in these penetration teams?

Inman: No, and I have great skepticism of the story, but I can't rule out that some of it is true because in the early 70s I was off doing totally different things. I had NSA from July 1977 to March 1981. That's when we began some of our concentrated efforts on computer security. But it was not touched off by any of these teams at all: It was getting at a multilevel security problem.

A point that ought to be made is the vast majority of the networking of military computers where you are dealing with operational information, . . . they're classified. They're enciphered communications streams already so the amateur in fact can't penetrate them. They could jam them, that could keep them from working, but they could not access the data base. So you have two different kinds of networks. You've got research networks that are unclassified that are easy to penetrate, and you've got the classified where encipherment devices, at great expense, cover the linkages, and those are not accessible to the "WarGames" kind of guys who dial up.

When you say you were working on multilevel security, do you mean internal security?

Inman: I mean different levels of classification within the same computer.

Were you more concerned about internal or external attack?

Inman: Internal.

Did you have computers that networked out to others?

Inman: Yes. Lots, all with fully enciphered communications and (I was) completely comfortable about their absolute security.

Have the Soviets penetrated a supercomputer in England? Do you know anything about that?

Inman: No. Again, that's unclassified research. Again, there is an information exchange group that was set up in Vienna; Kosygin's son-in-law was one of the principle officials. And it worked as a gateway. You could dial into that organization and through it access any number of unclassified research activities in Western Europe . . . The gate the other way did not access any Soviet computers . . . Again (there's the) need to separate unclassified research where you deliberately want widespread exchange among scientists . . . as opposed to government networks that are classified where you have already enciphered devices controlling all the external linkages. There the vulnerability is not the external access, it's the internal access.

Given the fact that that's true, is there any way that highly sensitive information—whether it's corporate information or government information—can ever be totally insured against attack?

Inman: It can be with enciphered devices, but most of those are very expensive, and many corporations have elected not to provide this protection of proprietary data. It's a big expense in the absence of hard evidence that anyone is listening . . . It's an economic question. As a reference point, you could go to a first-rate study done at Carnegie-Mellon University about three years ago by the College of Engineering and the College of Public Policy, in which they went out and interviewed a large number of business executives. The answer back was, there were very few companies that didn't spend the money where they were very concerned about proprietary data of value to their competitors, but the overwhelming majority, in the absence of certainty that insulation (of what) they were transmitting wasn't going to help the competitor, weren't willing to pay the cost.

The multilevel security is an entirely different argument. That is, we buy computers that have enormous capacity. Can you store in those computers various levels of information: unclassified, confidential, secret, top secret, and limit access only to people who are authorized to access that (level) of data? That is a very tough problem. But if you want to get maximum use of the computers, instead of having to buy different ones for different purposes, it's one that would be economically very desirable to solve.

Does NSA have a satisfactory system of multilevel security?

Inman: They're still compartmenting it off.

Do you think multilevel security will be possible in the future?

Inman: I think it will be.

But it isn't at the moment?

Inman: No.

Which computer systems are secure in your eyes?

Inman: Most of the ones in use. In the government at this point I'd be very comfortable for their complete security from unauthorized access to the classified facility.

Internal attack is still a problem?

Inman: Internal attack will always be a problem.

What direction will corporations and governments take in the future to make sure their computers are safe?

Inman: There are always a lot of things major corporations like banks are doing. Limiting physical access, plastic cards required for access. All kinds of checks. You have a whole variety of things in place now, and I suspect there will be more over time depending on the challenge. On the larger question, is there going to be a market for transmission protection of proprietary data? That depends on whether the corporations ultimately conclude they are being pursued by competitors.

What has been the Japanese reaction to your announcements? Are they following this?

Inman: I'm told that they're following this very closely, and there's a lot of talk about it. But I haven't any direct contact, so I can't give you a first-hand reaction.

I have great admiration for Dr. William O. Baker, the former head of Bell Labs. In an interview, he proposed a sort of Japanese-U.S. collaboration on this project. My response is: I don't rule out ultimate collaborative efforts but I think they'll have to be tri-lateral: Western Europe and Japan as well as the U.S. I don't think we can join up with Japan to take on Western Europe any more than we could join with Western Europe to take on Japan. We've got to find a way, ultimately, to keep all those relationships open . . . I believe it's achievable provided *you've* got the technology they want.

They have the technology we want now? Japan?

Inman: The Japanese certainly now have ceramic production techniques . . . I guess the answer to your question when you stand up and think about it is that the Japanese have been faster to go to the marketplace with new technology.

EXCERPTED